REMARKS/ARGUMENTS

The Office Action mailed March 22, 2005 has been reviewed and carefully considered. Claims 64-74 are canceled. Claims 1, 24, and 47 have been amended. Claims 1-63 are pending in this application, with claims 1, 24, and 47 being the only independent claims. Reconsideration of the above-identified application, as herein amended and in view of the following remarks, is respectfully requested.

In the Office Action mailed March 22, 2005, claims 1, 21-24, 44-47, 61-64, and 73-74 stand rejected under 35 U.S.C. §102(e) as anticipated by U.S. Patent Application Publication No. 2003/0078058 (Vatanen).

Claims 2, 25, 48, 65, and 66 stand rejected under 35 U.S.C. §103 as unpatentable over Vatanen.

Claims 3, 4, 9, 16, 26, 27, 32, 39, 49, 52, and 67 stand rejected under 35 U.S.C. §103 as unpatentable over Vatanen in view of 3GPP Technical Specification 3G-TS-33.203, Access Security for IP-Based Services (3G-TS-33.203).

Claims 5-8, 28-31, 50 and 51 stand rejected under 35 U.S.C. §103 as unpatentable over Vatanen in view of 3G-TS-33.203 and further in view of 3GPP Technical Specification 3G-TS-33.102, Security Architecture (3G-TS-33.102).

Claims 10-15, 17-20, 33-38, 40-43, 53-60, and 68-72 stand rejected under 35 U.S.C. §103 as unpatentable over Vatanen in view of 3G-TS-33.203 and further in view of U.S. Patent Application Publication No. 2002/0103850 (Moyer).

SUMMARY OF PRESENT APPLICATION

Before discussing the cited prior art and the Examiner's rejections of the claims in view of that art, a brief summary of the subject matter described in the present application is

appropriate and will facilitate an understanding of the arguments below which distinguish the claimed invention from the prior art. The present application relates to a method and device for providing confidentiality protection in a session initiation protocol (SIP) messages sent from a user equipment (UE) to a network element, i.e., a proxy-Call Session Control Function (p-CSCF). As explained in the background section of the present application, a problem with SIP messages is that the header must remain unencrypted so that the messages can be properly routed (see page 3, lines 2-7 of the application). However, this allows the sender's identification in the header to be read by anyone who captures or inadvertently receives the message. To overcome this problem, a temporary identity index is created using a secret key and algorithm known to the sender and receiver and public information identifying the sender of the message (page 4, lines 7-9). The temporary identity index is then inserted in a header field of a SIP message in place of a Uniform Resource Identifier (URI) for providing the sender's identity (page 4, lines 13-15). Both the user equipment and the network element separately determine the temporary identity index during registration of the user equipment before starting a session (page 7, lines 2-4; page 7, lines 16-18; and page 8, lines 5-6).

ARGUMENTS

Each of the independent claims 1, 24, and 47 is amended to recite that the temporary identity index is calculated separately in each of the user equipment and network element.

Vatanen discloses a method for transmission of secure messages in a telecommunication network. According to Vatanen a header section of the message includes a Mobile User Identification (MUI) (Pidkey) formed using a hash function and a public name (see paragraph 0021 of Vatanen). Vatanen applies to a broad range of messages used in telecommunication networks (see paragraph 0005). In paragraph 0019 Vatanen discloses that the

MUI Pidkey identifies the public signing key that is to be used to decrypt and verify the signature. However, Vatanen fails to disclose that the MUI (Pidkey) is separately generated at both the receiver and sender before the message is sent, as is now expressly recited in independent claims 1, 24, and 47. In fact, Vatenen fails to disclose that the MUI (Pidkey) is calculated at the receiver.

In view of the above amendments and remarks, independent claims 1, 24, and 47 are not anticipated by Vatanen under 35 U.S.C. §102. Furthermore, Vatenen fails to teach or suggest that the MUI Pidkey could be determined by both the sender and receiver before the message is sent because the MUI Pidkey includes information identifying which public key to use to decrypt the message. Accordingly, independent claims 1, 24, and 47 are also allowable over Vatanen under 35 U.S.C. §103.

Dependent claims 2-23, 25-46, and 48-63, each being dependent on one of independent claims 1, 24, and 47, are deemed allowable for at least the same reasons expressed above with respect to independent claims 1, 24, and 47.

Dependent claims 8 and 31 each further recite that the temporary identity index is stored in a memory in a visiting network. Vatanen fails to disclose this limitation because Vatanen discloses that the MUI Pidkey includes information identifying which public key to use to decrypt the message. Since the MUI Pidkey includes the information required to decrypt, a visiting network is not required to store the MUI Pidkey. Accordingly, independent claims 8 and 31 are allowable over Vatanen for at least these additional reasons.

The application is now deemed to be in condition for allowance and notice to that effect is solicited.

Respectfully submitted,
COHEN, PONTANI, LIEBERMAN & PAVANE

By _____

Alfred W. Froebrich
Reg. No. 38,887
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: July 21, 2005